JOURNAL OF ALGEBRA **144**, 359–370 (1991)

Corestriction of Galois Algebras

CARL HANS WENNINGER

Mathematisches Institut der Universität München, Theresienstrasse 39, D-8000 Munich 2, Germany

Communicated by Nathan Jacobson

Received July 25, 1989

INTRODUCTION

When studying invariants of fields, one is usually interested in the behaviour of these invariants under field extensions. In case of the Brauer group for example, there are two important maps relating $\mathrm{Br}(K)$ and $\mathrm{Br}(L)$ in the case of a finite, separable extension L/K: the restriction $\mathrm{Res}_{L/K}: \mathrm{Br}(K) \to \mathrm{Br}(L)$ and the corestriction $\mathrm{Cor}_{L/K}: \mathrm{Br}(L) \to \mathrm{Br}(K)$. The latter is usually defined in terms of Galois cohomology, but Riehm [13] gave a purely algebra-theoretic definition by assigning to every L-algebra A a K-algebra $\mathrm{Cor}_{L/K}(A)$ in a functorial manner.

In this paper we study Riehm's corestriction for algebras carrying a Galois structure with respect to a finite dimensional Hopf algebra. This concept of Galois algebras was introduced by Chase and Sweedler [2] in the case of commutative algebras. There are many examples [8]; the first two that come to mind are the classical one, in which a finite group operates by automorphisms, and the case of fully G-graded algebras for a finite group G [5, 1.5].

However, it turns out that the concept of group-Galois or fully graded algebras is too restrictive when one is studying the corestriction of such algebras. This is because if A is an H-Galois algebra over L, its corestriction is a Galois algebra with respect to the corestriction of H, which is not a group ring, even if H is. This happens, for example, in the case of norm residue algebras, the corestrictions of which were recently studied by Merkurjev [11] in the search for a set of nice generators for the Brauer group. We will study the corestriction of such algebras, which are smash products of two commutative Galois algebras with respect to a Hopf algebra and its dual, in a subsequent paper, where we will derive a generalization of the projection formula for cyclic algebras [16].

There is, however, a somewhat different corestriction for Galois algebras

0021-8693/91 $3.00

with respect to a *fixed* Hopf algebra H, provided H is cocommutative (this corresponds to the case of abelian Galois groups) and is defined over K. We call this corestriction the H-norm. The name "norm" is justified by examples, in which the H-norm can be interpreted as the classical norm resp. trace of elements of L, and by the above-mentioned generalization of the projection formula, where the H-norm replaces the classical norm.

Before we study the corestriction of Galois algebras in Section 2, we first deal with the behaviour of Galois algebras under change of the Hopf algebra, which does not seem to appear in the literature in this generality.

This paper constitutes part of the author's thesis [18], which was written under the guidance of Professor Pareigis. Part of the work for this thesis was done at Cornell University, and the author is indebted to Professor Chase and Professor Sweedler for their continuous interest and their valuable suggestions.

1. Galois Algebras and Functoriality

Let k be a commutative ring, $\otimes = \otimes_k$. All Hopf algebras are assumed to be finitely generated projective k-modules. We use the notation of [15] for Hopf algebras and comodules, except that we denote the multiplication map of a Hopf algebra by ∇. In particular S denotes the antipode.

Definition 1. Let H be a Hopf algebra over k. An H-comodule algebra $\alpha: A \to A \otimes H$ (i.e., A is a k-algebra and the H-comodule structure map α is an algebra map) is called an *H-Galois algebra* if A is faithfully flat over k and the canonical map $\tilde{\alpha}: A \otimes A \to A \otimes H$ sending $a \otimes b$ to $(a \otimes 1) \cdot \alpha(b)$ is bijective.

For an arbitrary H-comodule algebra A the map $\tilde{\alpha}: {}_{.}A \otimes A^{\cdot} \to {}_{.}A \otimes H^{\cdot}$ is left A-linear and right H-colinear, where the lower resp. upper dots indicate the module resp. the comodule structures we are talking about. Furthermore, $\tilde{\alpha}$ is multiplicative if and only if A is commutative. Hence, if A is a commutative H-Galois algebra, H must be commutative as well.

Basic examples of Galois algebras include Galois extensions in the sense of Chase, Harrison, and Rosenberg, fully graded algebras, and classes of Azumaya algebras like the cyclic algebras [1].

A morphism between two H-comodule algebras A and B is by definition an H-colinear algebra map. If A and B are two Galois algebras, we call such a map an *H-Galois morphism* for short. We denote by $\mathrm{Gal}(H)$ resp. $\mathrm{Gal}_c(H)$ the sets of isomorphism classes of H-Galois resp. of commutative H-Galois algebras.

The following fact is well known:

LEMMA 1. *In the category of H-Galois algebras every morphism is an isomorphism.*

Proof. Every H-Galois morphism $f\colon A \to B$ induces a commutative square

$$\begin{tikzcd} A\otimes A \arrow[r, "\sim"] \arrow[d, "f\otimes f"] & A\otimes H \arrow[d, "f\otimes 1"] \\ B\otimes B \arrow[r, "\sim"] & B\otimes H \end{tikzcd}$$

Reducing to the case of a ground field and counting ranks yields the claim. ▮

Now suppose $\varphi\colon G \to H$ is a Hopf algebra map. φ induces a forgetful functor $\mathscr{F}_\varphi$, which assigns to a G-comodule algebra $A \to A\otimes G$ the H-comodule algebra $A \to A\otimes G \to A\otimes H$, where the last arrow is $1\otimes\varphi$. This functor has a right adjoint, which is given by the cotensor product: If $\beta\colon B \to B\otimes H$ is a right H-comodule algebra, then

$$B \,\square_H\, G = \{x \in B\otimes G \mid (\beta\otimes 1)(x) = (1\otimes\rho)(x)\}$$

is a G-comodule algebra, the diagonal being induced by the diagonal of G. Here $\rho = (\varphi\otimes 1)\circ\Delta\colon G \to H\otimes G$ denotes the left H-comodule algebra structure of G. The adjunction morphisms $\mathscr{F}_\varphi(B \,\square_H\, G) \to B$ resp. $A \to \mathscr{F}_\varphi(A) \,\square_H\, G$ are induced by the maps $1\otimes\varepsilon\colon B\otimes G \to B$ resp. by the diagonal map of A.

PROPOSITION 2. *If B is an H-Galois algebra, then $B \,\square_H\, G$ is a G-Galois algebra.*

Proof. Denote $A = B \,\square_H\, G$ and let α be its diagonal map. Consider the following chain of left B-linear isomorphisms:

$$\begin{aligned} B\otimes(B \,\square_H\, G) &\cong (B\otimes B) \,\square_H\, G \\ &\cong (B\otimes H) \,\square_H\, G \\ &\cong B\otimes(H \,\square_H\, G) \\ &\cong B\otimes G. \end{aligned}$$

Call it ψ (the last isomorphism in this chain is induced by $(\varphi\otimes 1)\circ\Delta\colon G \xrightarrow{\sim} H \,\square_H\, G$). Then $\psi(\sum b\otimes b'\otimes g) = \Sigma\, b\cdot b'\otimes g$. A is k-faithfully flat, since B and G are. We have to show that $\tilde{\alpha}$ or equivalently $B\otimes\tilde{\alpha}$ is bijective. As to this consider the commutative diagram (τ the twist map)

$$\begin{tikzcd}
B\otimes(B\,\square_H G)\otimes(B\,\square_H G) \arrow[r, "B\otimes\tilde{\alpha}"] \arrow[d, "\psi\otimes 1"] & B\otimes(B\,\square_H G)\otimes G \arrow[dd, "\psi\otimes 1"] \\
B\otimes G\otimes(B\,\square_H G) \arrow[d, "(1\otimes\tau)(\psi\otimes 1)(1\otimes\tau)"] & \\
B\otimes G\otimes G \arrow[r, "1\otimes\tilde{\Delta}"] & B\otimes G\otimes G
\end{tikzcd}$$

Now $\tilde{\Delta}$ is bijective (G is a G-Galois algebra), and the claim follows. ∎

DEFINITION 2. Let $\varphi: G\to H$ be a Hopf algebra map, $A\in \mathrm{Gal}(G)$, and $B\in \mathrm{Gal}(H)$. An H-comodule algebra map $f: \mathscr{F}_\varphi(A)\to B$ is called a *φ-Galois morphism* for short. This amounts to saying that $f: A\to B$ is an algebra map which is *φ-colinear*, i.e., the diagram

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[d, "\beta"] \\
A\otimes G \arrow[r, "f\otimes\varphi"] & B\otimes H
\end{tikzcd}$$

commutes.

This definition is justified by the following fact:

THEOREM 3. *If $\varphi: G\to H$ is a morphism of finite Hopf algebras, then for every $B\in \mathrm{Gal}(H)$ there is a uniquely determined $A\in \mathrm{Gal}(G)$ on which there can be defined a φ-Galois morphism $f: A\to B$. Setting $\mathrm{Gal}(\varphi)(B)=A$ makes $\mathrm{Gal}(-)$ a contravariant, set valued functor on the category of finite Hopf algebras. If both G and B are commutative, then so is A. Hence, on the category of finite, commutative Hopf algebras, $\mathrm{Gal}_c(-)$ is a subfunctor of $\mathrm{Gal}(-)$.*

Proof. $A=B\,\square_H G$ is in $\mathrm{Gal}(G)$ and the adjunction morphism is a φ-Galois morphism from A to B. Suppose $f': A'\to B$ is another φ-Galois morphism. By the universal property of A stemming from the adjointness of $\mathscr{F}_\varphi$ and $-\square_H G$, there is a G-comodule algebra map $g: A'\to A$ with $f'\circ g=f$. By Lemma 1, g is an isomorphism, and hence $A=A'$ in $\mathrm{Gal}(G)$. ∎

Remark. The above theorem is analogous to a well-known fact in the theory of group extensions: Suppose $1\to M\to B\to H\to 1$ is a central extension of the abelian group M by a group H and $\varphi: G\to H$ is a group homomorphism. Then there exists a unique central extension $1\to M\to$

$A \to G \to 1$ such that there is a homomorphism $f\colon B \to A$ rendering the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & B & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & M & \longrightarrow & A & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

commutative. This analogy is not too surprising since Chase [1] has shown that for a commutative and cocommutative Hopf algebra H one can associate to every H-Galois algebra A a central extension (in a suitable Grothendieck topology) of the multiplicative group scheme by the Cartier dual of the group scheme represented by H and vice versa.

From Theorem 3 we can easily derive the existence of a group structure on $\mathrm{Gal}(H)$ in the case where H is cocommutative, which in a rather special case was first realized by Hasse [10].

COROLLARY 4. *For a cocommutative Hopf algebra H the set* $\mathrm{Gal}(H)$ *becomes an abelian group under* $A * B = \mathrm{Gal}(\Delta)(A \otimes B)$. $H = \mathrm{Gal}(\varepsilon)(k)$ *is the neutral element and* $(A^{\mathrm{op}}, (1 \otimes S) \circ \alpha)$, *where* A^{op} *denotes the opposite algebra of* A, *is the inverse of* $(A, \alpha) \in \mathrm{Gal}(H)$. *If H is also commutative,* $\mathrm{Gal}_c(H)$ *is a subgroup of* $\mathrm{Gal}(H)$.

Proof. We start with the general observation that if $A_i \in \mathrm{Gal}(H_i)$ $(i = 1, 2)$ then $A_1 \otimes A_2 \in \mathrm{Gal}(H_1 \otimes H_2)$. Now let $A, B \in \mathrm{Gal}(H)$. Since H is cocommutative, Δ is a Hopf algebra map and hence $*$ is well-defined. $\tau \circ \Delta = \Delta$ implies the commutativity of $*$. The diagonal $A \to A \otimes H$ is a Δ-Galois morphism and hence H is a neutral element. To show that A^{op} is an H-Galois algebra which is inverse to A, we have to work somewhat harder: Denote $\alpha^{\mathrm{op}} = (1 \otimes S) \circ \alpha\colon A^{\mathrm{op}} \to A^{\mathrm{op}} \otimes H$. This map makes A^{op} an H-comodule algebra. Let $g\colon A^{\mathrm{op}} \to A$ denote the identity map on the k-module A. The bijectivity of $\widetilde{\alpha^{\mathrm{op}}}$ follows from the commutative diagram

$$\begin{array}{ccc} A^{\mathrm{op}} \otimes A^{\mathrm{op}} & \xrightarrow{\widetilde{\alpha^{\mathrm{op}}}} & A^{\mathrm{op}} \otimes H \\ \downarrow{\scriptstyle \tau \circ (g \otimes g)} & & \downarrow{\scriptstyle \psi \circ (g \otimes 1)} \\ A \otimes A & \xrightarrow{\tilde{\alpha}} & A \otimes H \end{array}$$

where $\psi(\sum a \otimes h) = \sum a_{(0)} \otimes h \cdot a_{(1)}$ is bijective with inverse $\psi^{-1}(\sum a \otimes h) = \sum a_{(0)} \otimes h \cdot S(a_{(1)})$. Let f denote the composed map

$$f\colon H \xrightarrow{\ \imath\ } A \otimes H \xrightarrow{\tilde{\alpha}^{-1}} A \otimes A \xrightarrow{g^{-1} \otimes 1} A^{\mathrm{op}} \otimes A,$$

where $\iota(h) = 1 \otimes h$. We have to show that f is a Δ-Galois morphism. Clearly $f(1) = 1$. Suppose $g, h \in H$ are given. Let $f(g) = \sum a_i \otimes b_i$ and $f(h) = \sum c_j \otimes d_j$. Then $\tilde{\alpha}(\sum c_j a_i \otimes b_i d_j) = \sum c_j a_i b_{i(0)} d_{j(0)} \otimes b_{i(1)} d_{j(1)} = \sum c_j 1 d_{j(0)} \otimes g d_{j(0)} = 1 \otimes gh$. Hence f is an algebra map. It is routine to check that $\tilde{\alpha}$ is $\tilde{\Delta}$-colinear; that is, the diagram

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\tilde{\alpha}} & A \otimes H \\ \Big\downarrow{\scriptstyle (1 \otimes \tau \otimes 1) \circ (\alpha \otimes \alpha)} & & \Big\downarrow{\scriptstyle (1 \otimes \tau \otimes 1) \circ (\alpha \otimes \Delta)} \\ A \otimes A \otimes H \otimes H & \xrightarrow{\tilde{\alpha} \otimes \tilde{\Delta}} & A \otimes H \otimes H \otimes H \end{array}$$

commutes. By the definition of α^{op} the map g is S-colinear. Hence f is φ-colinear with

$$\varphi \colon H \xrightarrow{j} H \otimes H \xrightarrow{\tilde{\Delta}^{-1}} H \otimes H \xrightarrow{S \otimes 1} H \otimes H$$

and $j(h) = 1 \otimes h$. But since $\tilde{\Delta}^{-1}(g \otimes h) = \sum gS(h_{(1)}) \otimes h_{(2)}$ we get $\varphi = \Delta$. ∎

Remark. For a commutative and cocommutative Hopf algebra H the set of Hopf algebra endomorphisms carries a ring structure, the addition being given by the convolution product $(\varphi * \psi)(h) = \sum \varphi(h_{(1)}) \cdot \psi(h_{(2)})$. It is sometimes handy to realize that $\mathrm{Gal}_c(H)$ is actually a right module over this ring via $A \cdot \varphi = \mathrm{Gal}(\varphi)(A)$. Using this module structure, one easily gets that $\mathrm{Gal}_c(H)$ is a torsion group of exponent dividing the exponent of H (i.e., the order of id_H under convolution), which in turn divides the rank of H, provided the latter is defined.

Proof. That $\mathrm{Gal}_c(H)$ is a right module over the Hopf algebra endomorphism ring of H is straightforward to check, having realized that for a commutative Galois algebra A we have $\mathrm{Gal}(\nabla)(A) = A \otimes A$. This is because the multiplication map of A is a ∇-Galois morphism from $A \otimes A$ to A. Hence $\mathrm{Gal}(\varphi * \psi)(A) = \mathrm{Gal}(\nabla \circ (\varphi \otimes \psi) \circ \Delta)(A) = \mathrm{Gal}(\Delta)(\mathrm{Gal}(\varphi \otimes \psi)(A \otimes A)) = \mathrm{Gal}(\Delta)(\mathrm{Gal}(\varphi)(A) \otimes \mathrm{Gal}(\psi)(A)) = \mathrm{Gal}(\varphi)(A) * \mathrm{Gal}(\psi)(A)$. ∎

Now let R and S be two commutative rings. We want to study the behaviour of Galois algebras under functors from R-**Mod** to S-**Mod**, which preserve the tensor products:

DEFINITION 3. A covariant functor $\mathscr{G} \colon R\text{-}\mathbf{Mod} \to S\text{-}\mathbf{Mod}$ together with a functorial *iso*morphism $\delta \colon \mathscr{G}(M) \otimes_S \mathscr{G}(N) \xrightarrow{\sim} \mathscr{G}(M \otimes_R N)$ and an *iso*-morphism of S-modules $\zeta \colon S \xrightarrow{\sim} \mathscr{G}(R)$ is called a *monoidal functor*, if $(\mathscr{G}, \delta, \zeta)$ forms a weakly monoidal functor in the sense of [12, pp. 125], i.e., if δ and ζ are compatible with the natural isomorphisms $M \otimes (N \otimes P) \cong (M \otimes N) \otimes P$, $M \otimes N \cong N \otimes M$, and $M \otimes R \cong M$.

Let $\mathscr{G}$ be a monoidal functor. Obviously, monoidal functors are designed to preserve algebraic structures like algebras and their modules, coalgebras and their comodules, Hopf algebras and their comodule algebras, etc. Pareigis [12, Theorem 17] shows that $\mathscr{G}(M)$ will be finitely generated projective, if M is. Hence we conclude:

COROLLARY 5. *If* $\alpha: A \to A \otimes_R H$ *is an* H*-Galois algebra over* R, *then* $\mathscr{G}(\alpha): \mathscr{G}(A) \to \mathscr{G}(A) \otimes_S \mathscr{G}(H)$ *is an* $\mathscr{G}(H)$*-Galois algebra over* S.

We denote the induced map $\mathrm{Gal}(R, H) \to \mathrm{Gal}(S, \mathscr{G}(H))$ also by $\mathscr{G}$. Clearly, if $\varphi: G \to H$ is a morphism of R-Hopf algebras, the diagram

$$\begin{array}{ccc} \mathrm{Gal}(R, H) & \xrightarrow{\mathscr{G}} & \mathrm{Gal}(S, \mathscr{G}(H)) \\ \downarrow{\scriptstyle \mathrm{Gal}(\varphi)} & & \downarrow{\scriptstyle \mathrm{Gal}(\mathscr{G}(\varphi))} \\ \mathrm{Gal}(R, G) & \xrightarrow{\mathscr{G}} & \mathrm{Gal}(S, \mathscr{G}(G)) \end{array}$$

commutes. Furthermore, if H is cocommutative, $\mathscr{G}$ is a group homomorphism.

2. CORESTRICTION OF GALOIS ALGEBRAS

Let L/K be a separable field extension of finite degree n. By imitating Riehm's [13] construction of the corestriction of algebras we define a covariant functor $\mathrm{Cor}_{L/K}$: L-**Mod** $\to$ K-**Mod**. We briefly review its definition, mainly to fix notation.

Let N be the normal closure of L over K and $\Gamma = \mathrm{Gal}(N/K)$. Let $\Delta = \mathrm{Gal}(N/L)$ and $\Sigma = \Gamma/\Delta$, viewed as a left Γ-set as usual. Let $[\ ]: \Sigma \to \Gamma$ be a transversal. Then for $\gamma \in \Gamma$, $\sigma \in \Sigma$ there is a unique element $(\gamma, \sigma) \in \Delta$ with $\gamma \cdot [\sigma] = [\gamma \cdot \sigma] \cdot (\gamma, \sigma)$.

Now let V be a vector space over L. Set

$$V^{(\Gamma:\Delta)} = \bigotimes_{\sigma \in \Sigma} {}^{[\sigma]}(N \otimes_L V) \qquad \left(\text{here } \otimes = \bigotimes_N\right), \tag{1}$$

where for an N-vector space W and $\gamma \in \Gamma$ the symbol ${}^{\gamma}W$ denotes the γ-conjugate of $N \otimes_L V$ [13, 4.2], i.e., the additive group W with γ^{-1}-twisted operation of N. Γ operates by semilinear automorphisms on $V^{(\Gamma:\Delta)}$ via

$$\gamma \cdot \left(\bigotimes_{\sigma} (r_\sigma \otimes v_\sigma) \right) = \bigotimes_{\sigma} ((\gamma, \sigma')\, r_{\sigma'} \otimes v_{\sigma'}) \qquad (\sigma' = \gamma^{-1} \cdot \sigma). \tag{2}$$

By Galois descent the Γ-invariant elements form a K-vector space, and we set $\mathrm{Cor}_{L/K}(V) = (V^{(\Gamma:\Delta)})^{\Gamma}$. Clearly $N \otimes \mathrm{Cor}_{L/K}(V)$ is canonically isomorphic to $V^{(\Gamma:\Delta)}$ and $L \otimes \mathrm{Cor}_{L/K}(V) \cong (V^{(\Gamma:\Delta)})^{\Delta}$.

As is easily verified, this functor preserves the tensor product [4, I.8, Lemma 8 and 10]; i.e., $\mathrm{Cor}_{L/K}$ is a monoidal functor in the sense of Definition 3. Therefore it preserves algebraic structures like algebras and coalgebras, and one can even deduce that $\mathrm{Cor}_{L/K}$ induces a homomorphism on the Brauer group [12, Theorem 20].

Before we study the corestriction of Galois algebras, we note the adjointness properties of $\mathrm{Cor}_{L/K}$:

PROPOSITION 6. *On the category of commutative algebras* $\mathrm{Cor}_{L/K}$ *is left adjoint; on the category of cocommutative coalgebras it is right adjoint to the extension of scalars* $L \otimes_K -$.

Proof. For a commutative L-algebra A the map

$$A \ni a \mapsto (1 \otimes a) \otimes \left(\bigotimes_{\sigma \neq \Delta} (1 \otimes 1) \right) \in A^{(\Gamma:\Delta)}$$

induces a homomorphism of L-algebras

$$\iota_A : A \to L \otimes_K \mathrm{Cor}_{L/K}(A) \cong (A^{(\Gamma:\Delta)})^{\Delta}$$

and for a commutative K-algebra B the twisted $n = [L:K]$-fold multiplication $(L \otimes_K B)^{(\Gamma:\Delta)} \to N \otimes_K B$, $\bigotimes_\sigma (r_\sigma \otimes b_\sigma) \mapsto \prod_\sigma [\sigma](r_\sigma \otimes b_\sigma)$ for $r_\sigma \otimes b_\sigma \in {}^{[\sigma]}(N \otimes_K B)$, induces a homomorphism of K-algebras

$$\mu_B : \mathrm{Cor}_{L/K}(L \otimes_K B) \to B.$$

Dually, for a cocommutative L-coalgebra C the counit map can be used to define a homomorphism of L-coalgebras

$$\pi_C : L \otimes_K \mathrm{Cor}_{L/K}(C) \cong (C^{(\Gamma:\Delta)})^{\Delta} \to C$$

and for a cocommutative K-coalgebra D the n-fold diagonal gives rise to a K-coalgebra homomorphism

$$\delta_D : D \to \mathrm{Cor}_{L/K}(L \otimes_K D).$$

These maps are obviously functorial and fulfill the condition for adjunction morphisms. ∎

We remark at this point that all we did so far works as well if one replaces L/K by any ring extension l/k such that there exists a group-Galois extension n with l occuring as the fix ring of some subgroup. However, we do not know whether there is a similar construction in case of a Hopf Galois extension L/K.

We now come back to Galois algebras. By Corollary 5, $\mathrm{Cor}_{L/K}$ induces a map

$$\mathrm{Cor}_{L/K}\colon \mathrm{Gal}(L, H) \to \mathrm{Gal}(K, \mathrm{Cor}_{L/K}(H)),$$

which is natural in the L-Hopf algebra H.

PROPOSITION 7. *This map is injective and induces an isomorphism*

$$\mathrm{Cor}_{L/K}\colon \mathrm{Gal}_c(L, H) \xrightarrow{\sim} \mathrm{Gal}_c(K, \mathrm{Cor}_{L/K}(H)).$$

Proof. We define a map backward by sending $A \in \mathrm{Gal}(K, \mathrm{Cor}_{L/K}(H))$ to $\Psi(A) = \mathrm{Gal}(\iota_H)(L \otimes_K A) \in \mathrm{Gal}(L, H)$. Although H need not be commutative, the "adjunction" morphism $\iota_H\colon H \to L \otimes_K \mathrm{Cor}_{L/K}(H)$ is a well-defined Hopf algebra map. We claim that the map Ψ is a left inverse of $\mathrm{Cor}_{L/K}$ on $\mathrm{Gal}(L, H)$. For, if A is an H-Galois algebra over L, $\iota_A\colon A \to L \otimes_K \mathrm{Cor}_{L/K}(A)$ is an ι_H-Galois morphism and hence $A = \Psi(\mathrm{Cor}_{L/K}(A))$.

For the second part of the proof we may assume that H is commutative, since otherwise both $\mathrm{Gal}_c(L, H)$ and $\mathrm{Gal}_c(K, \mathrm{Cor}_{L/K}(H))$ are empty. Let $A \in \mathrm{Gal}_c(K, \mathrm{Cor}_{L/K}(H))$ and $j\colon \Psi(A) \to L \otimes_K A$ be an ι_H-Galois morphism. Then $\mu_A \circ \mathrm{Cor}_{L/K}(j)\colon \mathrm{Cor}_{L/K}(\Psi(A)) \to A$ is a $\mu_{\mathrm{Cor}_{L/K}(H)} \circ \mathrm{Cor}_{L/K}(\iota_H)$-Galois morphism. But $\mu_{\mathrm{Cor}_{L/K}(H)} \circ \mathrm{Cor}_{L/K}(\iota_H) = \mathrm{id}_H$ and the claim follows. ∎

EXAMPLE. Let $\mathbb{H}$ be the algebra of quaternions over the reals. It is fully graded by the group $V_4 = \{1, \sigma, \tau, \sigma\tau\}$, where $\deg(i) = \sigma$ and $\deg(j) = \tau$; i.e., $\mathbb{H}$ is an $\mathbb{R}[V_4]$-Galois algebra. We define a descent datum on $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H}$ by $\gamma(z \otimes a) = \bar{z} \otimes u^{-1} \cdot x \cdot u$, where γ is the non-trivial element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and $u = i + j$. We have $\gamma(1 \otimes i) = 1 \otimes j$ and consequently the $\mathbb{R}$-algebra of γ-invariant elements (which turns out to be isomorphic to the matrix ring $M_2(\mathbb{R})$) is equipped with an H-Galois structure, where H is the non-trivial form of $\mathbb{R}[V_4]$ corresponding to the descent datum which interchanges σ and τ. In particular H can be identified with the corestriction of $\mathbb{C}[C_2]$. This shows that $\mathrm{Cor}_{\mathbb{C}/\mathbb{R}}\colon \mathrm{Gal}(\mathbb{C}, \mathbb{C}[C_2]) \to \mathrm{Gal}(\mathbb{R}, \mathrm{Cor}_{\mathbb{C}/\mathbb{R}}(\mathbb{C}[C_2]))$ is not surjective, since every C_2-fully graded algebra is commutative and so will be its corestriction.

Remark. Let $\Gamma' = \mathrm{Gal}(K_s/K)$ denote the absolute Galois group of K. Assigning to a separable, commutative K-algebra A the Γ'-set X_A of all algebra maps from A to K_s yields an antiequivalence of the categories of separable, commutative K-algebras and the finite, discrete sets on which Γ' acts continuously [17, 6.3]. If A is a commutative H-Galois algebra, where H and hence A are separable, then X_A becomes a principal homogenous space for the Γ'-group X_H. One may use this to derive the well-known bijection $\mathrm{Gal_c}(K, H) \cong H^1(\Gamma', X_H)$ [17, 17.8; 14, 1.5.2, Proposition 33].

Denote $\Delta' \subset \Gamma'$ as the absolute Galois group of L. Assigning to a continuous Δ'-set S of the Γ'-set $M_{\Gamma'}^{\Delta'}(S)$ of all continuous, Δ'-equivariant maps from Γ' to S defines a right adjoint to the forgetful functor. We conclude that for a commutative, separable L-algebra A we have $X_{\mathrm{Cor}_{L/K}(A)} \cong M_{\Gamma'}^{\Delta'}(X_A)$. For a separable L-Hopf algebra H the above proposition can be stated as $H^1(\Gamma', M_{\Gamma'}^{\Delta'}(X_H)) \cong H^1(\Delta', X_H)$, which is well known in Galois cohomology [14, I.5.8.b].

If one wanted to study H-Galois algebras for a fixed Hopf algebra H, one might be more interested in the following map:

DEFINITION 4. Let H be a cocommutative Hopf algebra over K and $A \in \mathrm{Gal}(L, L \otimes_K H)$ be a Galois algebra. Then

$$H\text{-}\mathrm{N}_{L/K}(A) = \mathrm{Gal}(\delta_H)(\mathrm{Cor}(A),) \in \mathrm{Gal}(K, H),$$

where $\delta_H\colon H \to \mathrm{Cor}(L \otimes_K H)$ denotes the adjunction morphism introduced above, is called the *H-norm* of A.

Clearly this norm map

$$H\text{-}\mathrm{N}_{L/K}\colon \mathrm{Gal}(L, L \otimes_K H) \to \mathrm{Gal}(K, H)$$

is functorial in the K-Kopf algebra H. In particular it is a homomorphism of abelian groups.

PROPOSITION 8. *For every commutative and cocommutative K-Hopf algebra H, the composed map*

$$\mathrm{Gal_c}(K, H) \xrightarrow{L \otimes_K -} \mathrm{Gal_c}(L, L \otimes_K H) \xrightarrow{H\text{-}\mathrm{N}_{L/K}} \mathrm{Gal_c}(K, H)$$

equals multiplication by $n = [L : K]$.

Proof. For $A \in \mathrm{Gal_c}(K, H)$ the map $\mu_A\colon \mathrm{Cor}(L \otimes_K A) \to A$ is a μ_H-Galois morphism; i.e., $\mathrm{Cor}(L \otimes_K A) = \mathrm{Gal}(\mu_H)(A)$. Hence $H\text{-}\mathrm{N}_{L/K}(L \otimes_K A) = \mathrm{Gal}(\delta_H) \circ \mathrm{Gal}(\mu_H)(A) = \mathrm{Gal}(\mu_H \circ \delta_H)(A)$. But $\mu_H \circ \delta_H$ equals the n-fold convolution product of id_H in the Hopf algebra endomorphism ring of H (which is commonly denoted by $[n]$), and the claim follows from the fact that $\mathrm{Gal_c}(H)$ is a right module over this ring. ∎

EXAMPLES. 1. Let $H = K[C_r]$ be the group ring of the cyclic group of order r with generator τ. The H-Galois algebras are precisely the fully graded algebras $K[X]/(X^r - a)$, where a is a unit in K and $\deg(\bar{X}) = \tau$. By abuse of notation we write $K[\sqrt[r]{a}]$ for this algebra. For a unit a in L we then have $H\text{-}\mathrm{N}_{L/K}(L[\sqrt[r]{a}])=K[\sqrt[r]{b}]$, where b denotes the usual norm of a.

2. Let $H=K^{C_r}$ be the coordinate ring of the constant group scheme and suppose that L contains an rth primitive root of unity ζ. Let $t: \Gamma=\mathrm{Gal}(N/K) \to U(\mathbb{Z}/r\mathbb{Z})$ be the group homomorphism defined by $\gamma(\zeta)=\zeta^{t(\gamma)}$. By Kummer theory every $L \otimes_K H$-Galois algebra is of the form $L[\sqrt[r]{a}]$ for some unit a in L (here the fixed generator τ of C_r acts by $\tau(\bar{X})=\zeta \cdot \bar{X}$). It is straightforward to check that $L \otimes_K H\text{-}\mathrm{N}_{L/K}(L[\sqrt[r]{a}]) \cong L[\sqrt[r]{T_{L/K}(a)}]$, where

$$T_{L/K}(a)=\prod_{\sigma \in \Sigma} [\sigma]^{-1}(a)^{t([\sigma])}$$

is sometimes called the Stickelberger norm of a. This norm map was studied by Childs [3] and intensely used by Greither [7].

3. Finally let $H=K[T]/(T^q)$ be the coordinate ring of the group scheme α_q, where K is a field of characteristic $p>0$ and $q=p^r$. Again the corresponding Galois algebras are all commutative and isomorphic to $K[\sqrt[q]{a}]$, but this time a may be any element of K. For $a \in L$ we have $H\,\mathrm{N}_{L/K}(L[\sqrt[q]{a}])=K[\sqrt[q]{\mathrm{Tr}_{L/K}(a)}]$, where $\mathrm{Tr}_{L/K}(a)$ is the trace of a in K.

REFERENCES

1. S. U. CHASE, On a variant of the Witt and Brauer groups, *in* "Brauer Groups, Evanston, 1975," Lecture Notes in Mathematics, Vol. 549, pp. 148–187, Springer-Verlag, New York/Berlin, 1976.
2. S. U. CHASE AND M. E. SWEEDLER, Hopf algebras and Galois theory, *in* "Lecture notes in Mathematics," Vol. 97, Springer-Verlag, New York/Berlin, 1966.
3. L. N. CHILDS, Cyclic Stickelberger cohomology and descent of Kummer extensions, *Proc. Amer. Math. Soc.* **90** (1984), 505–510.
4. P. K. DRAXL, Skew fields, *in* "London Math. Soc. Note Series," Vol. 81, Cambridge Univ. Press, Cambridge, 1983.
5. T. E. EARLY AND H. F. KREIMER, Galois algebras and Harrison cohomology, *J. Algebra* **58** (1979), 136–147.
6. G. GARFINKEL AND M. ORZECH, Galois extensions as modules over the group ring, *Canad. J. Math.* **22** (1968), 242–248.
7. C. GREITHER, "Cyclic Galois Extensions and Normal Bases," Habilitationsschrift, Universität München, 1988.
8. C. GREITHER AND B. PAREIGIS, Hopf Galois theory for separable field extensions, *J. Algebra* **106** (1987), 239–258.
9. D. K. HARRISON, Abelian extensions of commutative rings, *Mem. Amer. Math. Soc.* **52** (1965), 1–14.
10. H. HASSE, Die Multiplikationsgruppe der abelschen Körper mit fester Galois-Gruppe, *Hamb. Abh.* **16** (1949), 29–40.

11. A. S. MERKURJEV, On the structure of the Brauer group of fields, *Math. USSR Izv.* **27**; No. 1 (1986), 141–157.
12. B. PAREIGIS, Non-additive ring and module theory. IV. The Brauer group of a symmetric monoidal category, *in* "Brauer Groups, Evanston, 1975," Lecture Notes in Mathematics, Vol. 549, pp. 112–133, Springer-Verlag, New York/Berlin, 1976.
13. C. RIEHM, The corestriction of algebraic structures, *Invent. Math.* **11** (1970), 73–98.
14. J. P. SERRE, Cohomologie Galoisienne, *in* "Lecture Notes in Mathematics," Vol. 5, Springer-Verlag, New York/Berlin, 1973.
15. M. E. SWEEDLER, "Hopf Algebras," Benjamin, New York, 1969.
16. J.-P. TIGNOL, On the corestriction of central simple algebras, *Math. Z.* **194** (1987), 267–274.
17. W. C. WATERHOUSE, Introduction to affine group schemes, *in* "Graduate Text in Mathematics," Vol. 66, Springer-Verlag, New York/Berlin, 1979.
18. C. H. WENNINGER, "Galois-Algebren zu Hopf-Algebren und verallgemeinerte Quaternionen," Dissertation, Universität München, 1989.